

IC CARD SECURE PERSONALIZATION METHOD**Field of the Invention**

[0001] The present invention relates to an integrated circuit (IC) card that allows for specific personalization thereof. More specifically, the invention relates to a method for completing the manufacturing phases of an IC card, such as performing a final and secure personalization phase of a semi-finished IC card including a non-volatile memory in which the personalization data and information are stored in secret allocations.

[0002] In the following, reference will be made to an IC card for specific purpose applications, such as to telephones. Also, the term smart card is used as an alternative to IC card, but without limiting the scope of protection of the present invention.

Background of the Invention

[0003] Typically, IC card manufacturing steps include a set of phases each having a well defined purpose in terms of providing a specific characterization or functionality to the card. A first phase regards a functional configuration of the card while a last phase relates to a personalization phase. This personalization phase requires storing specific secret data and information in the smart card non-volatile memory to allow proper operation of the card in the designated application field.

[0004] The stored information identifies each smart card. The physical location in the non-volatile memory, where all data are stored, is an industrial secret of the manufacturer and is normally not within the scope of being standardized. As an example, the GSM communication standard defines the concept of authentication keys but does not standardize where the keys are to be stored on the card or the format representing and protecting such keys.

[0005] The methods for data storing should ensure secrecy of the memory location. In the IC card manufacturing steps, two different working states can also be distinguished that may be defined as ADMINISTRATIVE and SECURED.

[0006] In the ADMINISTRATIVE state a set of commands is available for the user or administrator to perform the functional configuration, accessing to each position in the smart card non-volatile memory. In the ADMINISTRATIVE state, free access to the memory ensures that the personalization process can be performed for storing all required data in known locations. The ADMINISTRATIVE state is also an intermediate state in which the smart card can stay for further production steps.

[0007] Only at the end of the production process will the smart card be placed in the SECURED state. The SECURED state is a final state in which the smart card is passed from the manufacturer to the customer. All secret data stored in the non-volatile memory of the card cannot be freely accessed anymore. If, for any reason, the personalization process is not performed by the manufacturer, it cannot be performed anymore.

[0008] FIG. 1 is a schematic view showing the action steps performed to reach the secured state from the

administrative state. These steps are performed by the same manufacturer. This situation may be considered a restriction for providing a semi-finished production by a smart card manufacturer, since the final personalization in the secured state cannot be performed outside the factory. Therefore, this is a strong limitation to the possibility of supplying outside a predetermined number of micro-modules, that is, unfinished IC cards not yet protected in the secured state.

[0009] In such a case, when the personalization process should be performed by another organization or company, the only possibility to implement the personalization phase would be that of disclosing industrial secrets regarding the memory locations and the manner in which the card stores secret data.

[0010] Any disclosure of industrial secrets obviously need to be avoided by any smart card manufacturer. A known approach for providing personalization of an IC card is disclosed in U.S. Patent No. 4,105,156 concerning an identification card with interior circuits and a memory for use in a credit or identification system.

[0011] This approach is specifically provided for bank services wherein a personal identification number, i.e., a PIN, is associated to a semi-finished IC card including a non-volatile memory portion. This personalization phase is performed by a user, generally a bank entity, by entering the PIN through a write/reader device of the IC card including an encoder. The PIN is fed into a memory through gates that are automatically destroyed so that the association between the card and the PIN can no longer be changed.

[0012] This hardware approach has the drawback that a wrong PIN or a wrong personalization code cannot be changed after the personalization enabling procedure is started. In other words, once the secret memory locations are used to store the personalization data, access to such memory locations is physically interrupted according to the teaching of the above U.S. patent.

[0013] Currently, personalization of IC cards are much more complex than a simple association of a PIN or code number. The hardware system disclosed in U.S. Patent No. 4,105,156 would not be appropriate in large volumes of data and/or information required for the personalization step. A wrong instruction provided during the personalization phase would render a large number of IC cards inoperable. This corresponds to high costs being supported by the final user.

[0014] Therefore, it would be highly desirable for the final user to implement a personalization phase that could be defined in all possible details up to the last step of the personalization phase without destroying the possibility to re-program such a personalization phase. At the same time, the manufacturer of the IC is interested in offering to the final user a product having secret memory locations available for the personalization phase.

Summary of the Invention

[0015] An object of the present invention is that of allowing implementation of the IC card personalization step outside the organization or company performing the IC card manufacturing, but allowing at the same time the personalization phase to be re-programmed if needed.

[0016] Another object of the present invention is that of allowing a correct and secure personalization phase to be performed by an organization or company not having access to information concerning the manner in which the card stores secret data.

[0017] According to a first embodiment of the personalization phase, a method comprises storing an algorithm in the non-volatile memory for processing data as a finite-state machine, and enabling an entity different from the card manufacturer to access the algorithm for storing all necessary data and information required by the personalization phase according to a designated application field of the IC card. A security authentication step may be performed before enabling the algorithm to receive the data and information.

[0018] The algorithm may be enabled to receive the data and information, which are stored in secret memory locations of the non-volatile memory portion according to a predetermined data structure and an access procedure hidden to the entity. The enabling phase of the algorithm is allowed in the case of an incorrectly enabled personalization phase.

Brief Description of the Drawings

[0019] The features and advantages of the personalization method according to the present invention will be disclosed in the following description given by way of non-limiting illustrative examples with reference to the drawings.

[0020] FIG. 1 is a schematic view showing the action steps performed to reach the secured state from the administrative state as performed by a same manufacturer according to the prior art;

[0021] FIG. 2 is a schematic view of an IC card system including integrated circuit portions implementing the method according to the present invention;

[0022] FIG. 3 is a schematic view of a personalization phase performed by an entity different from the manufacturer of the IC card according to the present invention;

[0023] FIG. 4 is a schematic view showing different personalization process steps based on the application field and involving different personalization commands or instructions and different memory locations for storing data according to the present invention;

[0024] FIG. 5 is a schematic view showing a finite-state machine stored in a non-volatile memory portion of the IC card of FIG. 2; and

[0025] FIG. 6 is a schematic view showing a JavaCard applet loaded into the IC card of FIG. 2 during an administrative phase.

Detailed Description of the Preferred Embodiments

[0026] With reference to the figures, and more specifically to the example of FIG. 2, an IC card 1 according to the present invention is schematically shown. The IC card 1 includes means (FIG. 4) for allowing a final personalization step to be performed by an organization or company different from the manufacturer of the card.

[0027] A method completes the manufacturing phases of an IC card for performing a final and secure personalization phase of a semi-finished IC card including a non-volatile memory portion in which personalization data and information are stored in secret allocations.

[0028] The IC card 1 may have the format and external shape of a common SIM card for mobile telephone applications. However, nothing prevents the IC card 1 from having a different shape or format as may be required by a specific application. The IC card 1 includes a conventional microcontroller 2 or microprocessor and conventional memory portions 3, 4 and 5 which are strictly associated with the microcontroller 2.

[0029] The microcontroller 2 and the associated memory portions may be an integrated embedded system equipped with a first read only memory portion 3, a second or extended non-volatile memory portion 4 and at least one additional memory portion 5.

[0030] The first memory portion 3 is generally a ROM memory including programs, i.e., software applications, masked on the read-only memory and defining the function of the IC card 1. The second and extended memory portion 4 is a non-volatile memory and may be an electrically erasable memory, such as an EEPROM or Flash normally having a NOR structure and including subroutines, extended instructions and/or customized data.

[0031] The additional memory portion 5 may be structurally and functionally independent from both the first read only memory portion 3 and the extended memory portion 4, and may be a read/write memory such as a volatile RAM. As an alternative, the additional memory portion 5 may also be an EEPROM or another non-volatile memory device.

[0032] The IC card 1 may be considered a semi-finished product since the final personalization phase is missing from the card. However, the IC card 1 includes means for allowing an external source

implementing this final personalization phase that depends on the application field. In other words, the application field involves different personalization commands or methods, and different memory locations on where to store secret data and information.

[0033] A method for performing the personalization phase on the smart card in the secured state is also provided. The method allows the smart card personalization phase to be performed by an organization or company not having access to information concerning the manner in which the card stores the secret data.

[0034] To do so, the method provides an abstract of the data stored in the non-volatile smart card memory portion. In other words, knowledge of the data location is hidden for the entity performing the final personalization phase.

[0035] The method is characterized by the following steps. An algorithm is stored in the non-volatile memory portion 4 for processing data as a finite-state machine 10. An entity different from the card manufacturer is enabled to access the algorithm for storing all necessary data and information required by the personalization phase, according to a designated application field of the IC card.

[0036] The algorithm is enabled to receive the data and information which are stored in memory locations of the non-volatile memory portion according to a predetermined data structure and an access procedure hidden to the entity. The memory location knowledge for the data storing is a prerequisite for allowing the operation to be performed. This knowledge depends on the application field, and it also characterizes the smart card product.

[0037] FIG. 3 shows the different personalization processes depending on the application field. The application field involves different personalization commands or methods, and different memory locations where the data is to be stored.

[0038] The different personalization commands corresponding to different memory locations on where to store data are included in the non-volatile memory portion. Moreover, personalization data are stored in the card during the personalization phase without any knowledge by the entity different from the card manufacturer about the location where the data will be stored. This is obtained by a process performed by the state machine 10 taking care of the data storing, but not showing any information about the data location. This provides a process independent from the smart card application field.

[0039] The method steps are identified by the processing of a finite-state machine 10 as shown in FIG. 5. A beginning state (IDLE state) corresponds to the SECURED state at the end of all personalization and end production steps.

[0040] The transitions from one state to another state may be activated by predetermined events that are listed as follows: Personalization Process Enabling, Security Authentication, Data Sending, and Personalization Completion.

[0041] Each event is triggered by a command sent to the smart card microprocessor 2. The commands are as follows, wherein the term PERSO means personalization: ENABLE PERSO, VERIFY PERSO CODE, PUT PERSO DATA, and LOCK PERSO.

[0042] At the beginning of the personalization process, the card 1 is in the IDLE state, ready for

receiving one of the above commands. This is the starting point for the personalization process, and the smart card will return to this initial state every time after a reset command, as shown in FIG. 4.

[0043] An ENABLE PERSO command allows the transition on the READY state. In this READY state the smart card 1 has been enabled to receive the commands specified for the data personalization. When the card 1 is in this READY state an authentication command shall be evaluated before sending data for security reasons. This is shown in FIG. 4 by the verify steps.

[0044] The READY state is a transition state, and only the VERIFY PERSO CODE command will be accepted. Upon receiving the right input code, the state will be changed in the PERSO state. While in case of receipt of a wrong code, the new state will be an ALERT state. The ALERT state is another transition state and only the VERIFY PERSO CODE command will be accepted.

[0045] Upon receiving the right input code the new PERSO state will be reached, but after some attempts receiving a wrong PERSO code the new state will be BLOCKED. The BLOCKED state is an irreversible state, and the smart card 1 cannot be personalized anymore and needs to be discharged.

[0046] After a VERIFY PERSO CODE is successfully performed, the PERSO state will be reached and the data can be sent to the smart card 1 through the PUT PERSO DATA commands. It could be possible to send a sequence of the PUT PERSO DATA command with different formats for the personalization completion.

[0047] When all the personalization data have been stored in the smart card non-volatile memory portion 4, the last command to send is the LOCK PERSO command. The LOCK PERSO state ends the personalization process, and

represents an irreversible software lock to the personalization data of the IC Card

[0048] The method may be based on a JavaCard applet loaded into the smart card 1 during the ADMINISTRATIVE phase, as schematically shown in FIG. 5. After the first LOCK the IC card 1 passes to the SECURED state. Then, the personalization data can be stored by the customer only via the personalization applet.

[0049] The personalization applet allows implementation of the steps described above, providing the abstract for the data being stored in the non-volatile smart card memory portion 4.

[0050] The method has the advantage of allowing the final user to implement a personalization phase that could be defined in all possible details up to the last step of the personalization phase without destroying the possibility to re-program such a personalization phase. At the same time the manufacturer of the IC card 1 may offer to the final user a product having secret memory locations available for the personalization phase.

[0051] The personalization phase is performed through commands that are able to access the secret memory locations without indicating specific additional parameters. These accesses reinforce the security policy of the smart card 1 because, not indicating specific additional parameters to access memory locations, is a significant improvement to mask the internal memory organization and file system of the smart card 1.

[0052] The algorithm that implements the described process is stored on the IC card 1 already compliant to the standards. The memory for storing the information may be referred to as a logical model. This model could

be a file system that is an abstraction of the memory physical layer.

[0053] The memory locations could be represented by all the available files, each one identified by the ID. The information are then stored in the files. The target is the file ID hiding during the personalization process of the semi-finished product performed by the user.

[0054] Furthermore, the information stored in the files have a typical format that needs to also be hidden to the entity that performs the personalization process. The algorithm loaded on the IC card 1 implements the described abstraction layer (file ID and file format hiding), managing only the data to store without reference to the file ID or any file body format.

[0055] The secure personalization process is also different from the prior art because it is reversible after each data storing. The process is finished, and not reversible, only if formally required (see LOCK PERSO command in FIG. 5). For this reason each data stored could be replaced, one or more times, before the formal request for ending the process.